PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2001-256191**

(43)Date of publication of application : **21.09.2001**

(51)Int.Cl. **G06F 15/00**
G06T 7/00

(21)Application number : **2000-064634**

(22)Date of filing : **09.03.2000**

(71)Applicant : **MITSUBISHI ELECTRIC CORP**

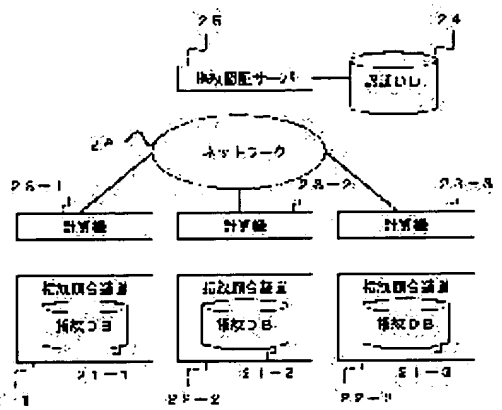
(72)Inventor : **SADAKANE TETSUO**
BABA YOSHIMASA
OKAZAKI NAONOBU
NAKAMURA HIROSHI
FUJII TERUKO

(54) NETWORK FINGERPRINT AUTHENTICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To reduce the loads of a network and an authentication server while unitarily managing authentication information.

SOLUTION: This system is provided with a fingerprint DB capable of preserving a user identifier and fingerprint information, a fingerprint collation device for collating an inputted user identifier and sampled fingerprint information with the fingerprint DB and outputting the sampled fingerprint information in the case that the collated result matches or in the case that the inputted user identifier is not preserved in the fingerprint DB, a computer for transmitting the authentication information including the fingerprint information outputted from the fingerprint collation device and the user identifier and requesting authentication, an authentication DB for preserving the authentication information including the user identifier and the fingerprint information registered beforehand and a fingerprint authentication server for collating the authentication information transmitted from the computer with the authentication DB and authenticating a fingerprint.



LEGAL STATUS

[Date of request for examination] 18.03.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－256191
（P2001－256191A）
(43)公開日　平成13年９月21日(2001.9.21)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｆ	５Ｂ０４３
Ｇ０６Ｔ　7/00		15/62	４６０	５Ｂ０８５

審査請求　未請求　請求項の数11　ＯＬ　（全 15 頁）

(21)出願番号　特願2000－64634(P2000－64634)

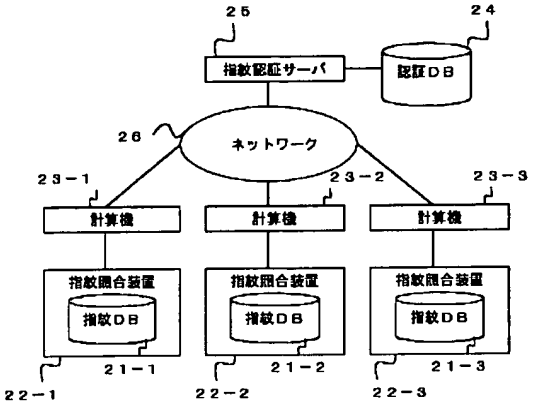
(22)出願日　平成12年３月９日(2000.3.9)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　貞包　哲男
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　馬場　義昌
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100102439
弁理士　宮田　金雄　（外１名）

最終頁に続く

(54)【発明の名称】　ネットワーク指紋認証システム

(57)【要約】
【課題】　認証情報の一元管理を行いながら、ネットワークと認証サーバの負荷軽減を実現する。
【解決手段】　使用者識別子と指紋情報とが保存可能な指紋ＤＢと、入力された使用者識別子と採取した指紋情報とを前記指紋ＤＢと照合し、その照合結果が一致した場合、又は、前記入力された使用者識別子が前記指紋ＤＢに保存されていない場合に、前記採取した指紋情報を出力する指紋照合装置と、前記指紋照合装置から出力された指紋情報とその使用者識別子とを含む認証情報を送信して認証依頼する計算機と、予め登録された使用者識別子と指紋情報とを含む認証情報が保存された認証ＤＢと、前記計算機から送信された認証情報と前記認証ＤＢと照合して指紋認証を行う指紋認証サーバとを備える。



1

【特許請求の範囲】

【請求項１】　使用者識別子と指紋情報とが保存可能な指紋ＤＢと、

入力された使用者識別子と採取した指紋情報とを前記指紋ＤＢと照合し、その照合結果が一致した場合、又は、前記入力された使用者識別子が前記指紋ＤＢに保存されていない場合に、前記採取した指紋情報を出力する指紋照合装置と、

前記指紋照合装置から出力された指紋情報とその使用者識別子とを含む認証情報を送信して認証依頼する計算機と、

予め登録された使用者識別子と指紋情報とを含む認証情報が保存された認証ＤＢと、

前記計算機から送信された認証情報と前記認証ＤＢと照合して指紋認証を行う指紋認証サーバとを備えたことを特徴とするネットワーク指紋認証システム。

【請求項２】　前記指紋照合装置は、前記指紋認証サーバでの指紋認証結果が認証成功であった場合で、かつ、その使用者識別子が前記指紋ＤＢに保存されていない場合に、前記入力された使用者識別子と採取した指紋情報とを前記指紋ＤＢに保存するように構成されたことを特徴とする請求項１に記載のネットワーク指紋認証システム。

【請求項３】　前記指紋照合装置での指紋照合のしきい値が、指紋認証サーバでの指紋照合のしきい値より低く設定されたことを特徴とする請求項１又は請求項２に記載のネットワーク指紋認証システム。

【請求項４】　前記指紋照合装置は、前記採取した指紋情報の前記指紋認証サーバでの指紋認証結果が認証成功である度に、当該採取した指紋情報を前記指紋ＤＢに保存するように構成されたことを特徴とする請求項１ないし請求項３のいずれかに記載のネットワーク指紋認証システム。

【請求項５】　前記指紋照合装置は、前記採取した指紋情報の前記指紋認証サーバでの指紋認証結果が認証失敗であった場合に当該採取した指紋情報と入力された使用者識別子とを前記指紋ＤＢに保存し、後に入力された使用者識別子が前記認証失敗となった使用者識別子である場合に前記保存した認証失敗であった指紋情報と後に採取した指紋情報とを照合し、一致する場合には当該後に採取した指紋情報を前記計算機に出力しないように構成されたことを特徴とする請求項１ないし請求項４のいずれかに記載のネットワーク指紋認証システム。

【請求項６】　前記計算機は、前記採取した指紋情報と前記指紋ＤＢに保存された指紋情報との照合度を使用者に提示可能に構成されたことを特徴とする請求項１ないし請求項５のいずれかに記載のネットワーク指紋認証システム。

【請求項７】　前記指紋照合装置は、前記指紋認証サーバに登録されている指紋情報が変更された場合に、前記

2

指紋ＤＢに保存されている指紋情報を削除するように構成されたことを特徴とする請求項１ないし請求項６のいずれかに記載のネットワーク指紋認証システム。

【請求項８】　前記指紋照合装置は、前記指紋ＤＢに保存された指紋情報を所定時間後に削除するように構成されたことを特徴とする請求項１ないし請求項７のいずれかに記載のネットワーク指紋認証システム。

【請求項９】　採取した指紋情報を出力する指紋照合装置と、

前記指紋照合装置から出力された指紋情報とその使用者識別子とを含む認証情報を送信して認証依頼する計算機と、

使用者識別子と指紋情報とが保存可能な指紋ＤＢと、

前記計算機から送信された認証情報に含まれた指紋情報とその使用者識別子とを前記指紋ＤＢと照合し、その照合結果が一致した場合、又は、前記入力された使用者識別子が前記指紋ＤＢに保存されていない場合に、前記認証情報を出力する指紋認証キャッシュ・サーバと、

予め登録された使用者識別子と指紋情報とを含む認証情報が保存された認証ＤＢと、

前記指紋認証キャッシュ・サーバから出力された認証情報と上記認証ＤＢと照合して指紋認証を行う指紋認証サーバとを備えたことを特徴とするネットワーク指紋認証システム。

【請求項１０】　前記指紋認証キャッシュ・サーバは、照合結果が一致しない場合に指紋認証結果として認証失敗を送信するように構成されたことを特徴とする請求項９に記載のネットワーク指紋認証システム。

【請求項１１】　前記計算機は、前記指紋認証結果に基づいてアプリケーションの制御を行うように構成されたことを特徴とする請求項１ないし請求項１０のいずれかに記載のネットワーク指紋認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、採取した指紋情報を用いて指紋認証を行うネットワーク指紋認証システムに関するものである。

【０００２】

【従来の技術】図９は例えば、特開平８－３２９０１０号公報に示された従来のネットワーク認証システムであり、認証処理を行う複数のコンピュータシステムが通信網を介して相互に接続されたコンピュータネットワークシステムにおいて、該当コンピュータシステムに認証処理のための情報がない場合のみ、ネットワークを介して他のコンピュータシステムに認証処理を依頼することにより、ネットワーク上のデータ通信効率を向上を可能にしたものである。

【０００３】図９の説明を行う。図９に示されるコンピュータネットワークシステムは、アクセス権の有無を判定するための照合処理を行う複数のコンピュータシステ

証情報を送信して認証依頼する計算機と、予め登録された使用者識別子と指紋情報とを含む認証情報が保存された認証ＤＢと、前記計算機から送信された認証情報と前記認証ＤＢと照合して指紋認証を行う指紋認証サーバとを備えたものである。

【００１５】また、つぎの発明に係るネットワーク指紋認証システムは、前記指紋照合装置は、前記指紋認証サーバでの指紋認証結果が認証成功であった場合で、かつ、その使用者識別子が前記指紋ＤＢに保存されていない場合に、前記入力された使用者識別子と採取した指紋情報とを前記指紋ＤＢに保存するように構成されたものである。

【００１６】また、つぎの発明に係るネットワーク指紋認証システムは、前記指紋照合装置での指紋照合のしきい値が、指紋認証サーバでの指紋照合のしきい値より低く設定されたものである。

【００１７】また、つぎの発明に係るネットワーク指紋認証システムは、前記指紋照合装置は、前記採取した指紋情報の前記指紋認証サーバでの指紋認証結果が認証成功である度に、当該採取した指紋情報を前記指紋ＤＢに保存するように構成されたものである。

【００１８】また、つぎの発明に係るネットワーク指紋認証システムは、前記指紋照合装置は、前記採取した指紋情報の前記指紋認証サーバでの指紋認証結果が認証失敗であった場合に当該採取した指紋情報と入力された使用者識別子とを前記指紋ＤＢに保存し、後に入力された使用者識別子が前記認証失敗となった使用者識別子である場合に前記保存した認証失敗であった指紋情報と後に採取した指紋情報とを照合し、一致する場合には当該後に採取した指紋情報を前記計算機に出力しないように構成されたものである。

【００１９】また、つぎの発明に係るネットワーク指紋認証システムは、前記計算機は、前記採取した指紋情報と前記指紋ＤＢに保存された指紋情報との照合度を使用者に提示可能に構成されたものである。

【００２０】また、つぎの発明に係るネットワーク指紋認証システムは、前記指紋照合装置は、前記指紋認証サーバに登録されている指紋情報が変更された場合に、前記指紋ＤＢに保存されている指紋情報を削除するように構成されたものである。

【００２１】また、つぎの発明に係るネットワーク指紋認証システムは、前記指紋照合装置は、前記指紋ＤＢに保存された指紋情報を所定時間後に削除するように構成されたものである。

【００２２】さらにまた、つぎの発明に係るネットワーク指紋認証システムは、採取した指紋情報を出力する指紋照合装置と、前記指紋照合装置から出力された指紋情報とその使用者識別子とを含む認証情報を送信して認証依頼する計算機と、使用者識別子と指紋情報とが保存可能な指紋ＤＢと、前記計算機から送信された認証情報に含まれた指紋情報とその使用者識別子とを前記指紋ＤＢと照合し、その照合結果が一致した場合、又は、前記入力された使用者識別子が前記指紋ＤＢに保存されていない場合に、前記認証情報を出力する指紋認証キャッシュ・サーバと、予め登録された使用者識別子と指紋情報とを含む認証情報が保存された認証ＤＢと、前記指紋認証キャッシュ・サーバから出力された認証情報と上記認証ＤＢと照合して指紋認証を行う指紋認証サーバとを備えたものである。

【００２３】また、つぎの発明に係るネットワーク指紋認証システムは、前記指紋認証キャッシュ・サーバは、照合結果が一致しない場合に指紋認証結果として認証失敗を送信するように構成されたものである。

【００２４】また、つぎの発明に係るネットワーク指紋認証システムは、前記計算機は、前記指紋認証結果に基づいてアプリケーションの制御を行うように構成されたものである。

【００２５】

【発明の実施の形態】実施の形態１．図１はこの発明の実施の形態１の全体的な構成を示すシステム構成図である。図において、２１－１～３は、使用者識別子と指紋情報とが保存可能な指紋ＤＢであり、ここでは指紋照合装置の内部に設置されている。また、予め使用者識別子と指紋情報とが保存されている。２２－１～３は、使用者の指紋情報を採取すると共に、入力された使用者識別子と採取した指紋情報とを前記指紋ＤＢ２１－１～３と照合し、その照合結果が一致した場合、又は、前記入力された使用者識別子が前記指紋ＤＢ２１－１～３に保存されていない場合に、前記採取した指紋情報を出力する指紋照合装置である。また、ここでは、指紋認証サーバでの指紋認証結果が認証成功であった場合で、かつ、その使用者識別子が前記指紋ＤＢ２１－１～３に保存されていない場合に、前記入力された使用者識別子と採取した指紋情報とを前記指紋ＤＢ２１－１～３に保存するように構成されている。

【００２６】２３－１～３は、前記指紋照合装置２２－１～３から出力された指紋情報とその使用者識別子とを含む認証情報を指紋認証サーバに送信して認証依頼する計算機であり、ここでは、指紋取得のための使用者への指示を行うと共に、使用者識別子を前記指紋照合装置２２－１～３に入力し、指紋認証サーバの指紋認証結果に基づいてアプリケーションの制御を行うように構成されている。

【００２７】２４は、予め登録された使用者識別子と指紋情報とを含む認証情報が保存された認証ＤＢである。ここでは、認証の対象となる使用者の使用者識別子や指紋情報や前記アプリケーションに対するアクセス制御情報等を管理するように構成されている。２５は、前記計算機２３－１～３から送信された認証情報と前記認証ＤＢ２４と照合し、その指紋認証結果を前記計算機２３－

１～３に送信する指紋認証サーバでる。２６は、前記指紋認証サーバ２５と複数の計算機２３－１～３とを接続するネットワークである。

【００２８】次に動作について図２を用いて説明する。まず、指紋照合装置２２は、計算機２３の指示により使用者から指紋情報の採取を行う（ステップＳ３１）。この時に、指紋情報を採取する使用者の使用者識別子も計算機２３より受取る。そして、上記の使用者識別子を用いて指紋ＤＢ２１にアクセスして該当使用者の指紋情報が保存されているかを判断する（ステップＳ３２）。指紋情報が保存されていない場合は、計算機２３にその採取した指紋情報を送信する（ステップＳ３４）。指紋情報が保存されている場合には、その保存されている指紋情報と採取した指紋情報を照合する（ステップＳ３３）。ステップＳ３３で、指紋照合が一致した場合には、採取した指紋情報を計算機２３に送信する（ステップＳ３４）。指紋照合が一致しない場合には、もう一度指紋情報の採取を行う（ステップＳ３１）。

【００２９】次に、計算機２３は、受信した指紋情報に使用者識別子等の認証に必要な情報を加えた認証情報を指紋認証サーバ２５に送信する（ステップＳ３５）。

【００３０】次に、指紋認証サーバ２５は、受信した認証情報と認証ＤＢ２４に保存されている認証情報を用いて認証を行う（ステップＳ３６）。認証成功の場合には、認証成功のレスポンスを計算機２３に送信する。認証失敗の場合には認証失敗のレスポンスを計算機２３に送信する。

【００３１】次に、計算機２３は、指紋認証サーバ２５のレスポンスが認証成功の場合、アプリケーションの実行をする（ステップＳ３７）。認証失敗の場合、ユーザに通知して終了する。

【００３２】次に、計算機２３でアプリケーションが実行された場合（ステップＳ３７）、指紋照合装置２２は、指紋ＤＢ２１に該当指紋情報が保存されているかを判断する（ステップＳ３８）。保存されている場合には、終了する。保存されていない場合には、採取した指紋情報と使用者識別子を指紋ＤＢ２１に保存する（ステップＳ３９）。

【００３３】以上のように、この実施の形態のネットワーク指紋認証システムによれば、指紋照合装置で指紋照合を行い、その指紋照合結果が一致した場合、又は、入力された使用者識別子が指紋ＤＢに保存されていない場合に、指紋認証サーバで指紋認証を行うようにしたことにより、指紋認証サーバへの送信回数を軽減でき、使用者の利便性の向上、指紋認証サーバの負荷軽減、ネットワークの通信負荷軽減を実現することができる。また、認証ＤＢで認証情報を一元管理することにより、管理コスト、認証情報の秘匿のセキュリティの向上が可能となる。また、既存の指紋認証サーバ側を変更する必要がなく、端末側（本実施の形態では計算機、指紋照合装置、指紋ＤＢ）だけの変更で適用可能である。また、最終的には指紋認証サーバが指紋認証の判断を行うので、認証精度の整合性を保つことができる。

【００３４】また、指紋認証サーバでの指紋認証結果が認証成功であった場合で、かつ、その使用者識別子が前記指紋ＤＢに保存されていない場合に、入力された使用者識別子と採取した指紋情報とを前記指紋ＤＢに保存するようにしたことにより、次回以降の指紋照合において、当該使用者の指紋照合を指紋照合装置で行うことができるので、指紋認証サーバの負荷軽減を実現することができる。また、既存の指紋認証サーバ側を変更する必要がなく、端末側だけの変更で適用可能である。

【００３５】また、計算機は、指紋認証サーバでの指紋認証結果に基づいてアプリケーションの制御を行うようにしたことにより、使用者に指紋認証結果に応じたアプリケーションを提供することができる。

【００３６】実施の形態２．以上の実施の形態１では、指紋認証サーバで指紋照合する前に、指紋照合装置で指紋照合を行い、指紋認証サーバでの指紋認証を成功しやすくするようにしたものである。通常、指紋照合では、所定のしきい値以上の照合度があった場合に、２つの指紋が一致するように判定する。次に、指紋認証サーバの指紋照合では一致するが、指紋照合装置の指紋照合では一致しないような指紋情報に対応できるように、指紋照合装置での指紋照合で一致するように、指紋照合装置での照合のしきい値を低くした実施の形態を示す。

【００３７】実施の形態１と同様に図１は、この発明の実施の形態２の全体的な構成を示すシステム構成図である。前述の実施の形態と同一部分の説明を省略する。この実施の形態では、指紋照合装置２２での指紋照合のしきい値（照合度のしきい値）が、指紋認証サーバ２５の照合度のしきい値より低く設定されている。すなわち、指紋認証サーバ２５のしきい値は、各指紋照合装置２２－１～３を一元管理するために設定されたしきい値であるのに対し、各指紋照合装置２２－１～３のしきい値は、前記指紋認証サーバ２５のしきい値より低くなるように、それぞれ個別に設定されたものである。

【００３８】次に、動作について図２を用いて説明する。まず、指紋照合装置２２は、計算機２３の指示により使用者から指紋情報の採取を行う（ステップＳ３１）。この時に、指紋情報を採取する使用者の使用者識別子も計算機２３より受取る。そして、上記の使用者識別子を用いて指紋ＤＢ２１にアクセスして該当使用者の指紋情報が保存されているかを判断する（ステップＳ３２）。指紋情報が保存されていない場合は、計算機２３にその採取した指紋情報を送信する（ステップＳ３４）。指紋情報が保存されている場合には、その保存されている指紋情報と採取した指紋情報を照合する（ステップＳ３３）。ステップＳ３３で、指紋照合が一致した場合には、採取した指紋情報を計算機２３に送信する

ム１１（１１－１～１１－３）が通信網１２を介して相互に接続されている。各コンピュータシステム１１にはそれぞれデータ縮退ユニット１３（１３－１～１３－３）を介し、使用者の身体的特徴（特徴データ）を計測する特徴計測ユニット１４（１４－１～１４－３）がそれぞれ接続されている。このデータ縮退ユニット１４により使用者の身体的特徴が電気信号として抽出される。各コンピュータシステム１１には、それぞれファイルシステム１５（１５－１～１５－３）が接続されている。このファイルシステム１５は、アクセス権の有無を判定するための照合処理の際に参照される登録特徴データ、及び処理対象となる各種ファイル・データが格納されている。尚、接続されるコンピュータシステムの数はこれに限定されない。

【０００４】次に動作について説明する。図１０及び図１１に示されるフローチャートを参照して、図９に示されるコンピュータネットワークシステムのファイルアクセス動作について述べる。

【０００５】図９に示されるコンピュータネットワークシステムにおいて、任意のコンピュータシステム１１でファイルのアクセス要求が発生すると、このコンピュータ１１では、特徴計測ユニット１４を用いて身体的特徴、例えば指の指紋等を入力するように要求する。ここで、使用者の指紋が特徴計測ユニット１４に置かれると、データ縮退ユニット１３により縮退された特徴データが抽出する（ステップＳ１１、Ｓ１２）。

【０００６】抽出された特徴データ（抽出特徴データ）は、アクセス要求の発生した日時や、パスワード等の使用者識別子に付加される（ステップＳ１３）。尚、日時やパスワード等の使用者識別子を付与せず、縮退された抽出特徴データのみを用いてもよい。

【０００７】次に、コンピュータシステム１１では、アクセス要求されたファイルがこのコンピュータシステム１１に接続されているファイルシステム１５に格納されているか否かを判定する（ステップＳ１４）。ここで、ファイルシステム１５にアクセス要求されたファイルが格納されている場合、ファイルシステム１５に格納されている登録特徴データと、前記抽出特徴データ及び使用者識別子が同一であるか調べるために照合処理を行う（ステップＳ１６）。一致する場合は、ファイルにアクセスし（ステップＳ１７）、一致しない場合は、ファイルアクセスが不可能である通知等を行った後、ファイルアクセス要求に応じた処理が終了する。

【０００８】前記ステップＳ１４において、ファイルシステム１５にアクセス要求されたファイルが格納されていない場合、コンピュータシステム１１は、アクセス要求するファイルのファイル名と共に前記抽出特徴データ及び使用者識別子を、通信網１２を介して他のコンピュータシステムに送信する（ステップＳ１８）。この後、抽出特徴データ等を送出した送り先のコンピュータシステムからの応答を受信し、アクセスの可否に応じて前述したような処理を行う（ステップＳ１９）。尚、後述するがアクセス可の場合、アクセス要求したファイルが送られるので、これをファイルシステム１５に格納する。

【０００９】次に、前記ステップＳ１８において送出された各種データを受信したコンピュータシステム１１の処理を図１１を参照して説明する。

【００１０】コンピュータシステム１１は、他のコンピュータシステムからアクセス要求のあったファイルのファイル名等と共に前記抽出特徴データ及び使用者識別子を受信すると（ステップＳ２１）、アクセス要求されているファイルが自コンピュータシステム１１に接続されているファイルシステム１５に接続されたファイルシステム１５に格納されているか否か判定する（ステップＳ２２）。ここで、ファイルシステム１５に要求されたファイルが格納されていない場合、この旨を要求元のコンピュータシステムに通知する（ステップＳ２３）。

【００１１】前記ステップ２２において、アクセス要求されたファイルがファイルシステム１５に格納されている場合、ステップＳ２１において受信した抽出特徴データ及び使用者識別子を用い、要求元の使用者にファイルアクセス権が有るか否かを決定するための照合処理を行う（ステップＳ２４、Ｓ２５）。照合結果が一致である場合は、アクセス要求されたファイルを送信し（ステップＳ２６）、照合結果が不一致である場合は、ファイルのアクセス権が無いことを要求元のコンピュータシステムに通知する（ステップＳ２７）。

【００１２】

【発明が解決しようとする課題】以上のように、従来のネットワーク指紋認証システムにおいては、ネットワークの負荷軽減、認証サーバの負荷分散を実現するために、認証処理を行う複数のコンピュータシステムをネットワークを介して相互に接続し、認証に必要な情報（認証情報）を分散管理していたため、認証情報の登録・削除・変更等の管理時に整合性を保つのが困難であり、場合によってはかえってネットワーク、認証サーバに負荷がかかってしまうという問題点があった。

【００１３】この発明は上記のような問題点を解決するためになされたもので、認証情報の一元管理を行いながら、ネットワークと認証サーバの負荷軽減を実現することを目的とする。

【００１４】

【課題を解決するための手段】この発明に係るネットワーク指紋認証システムは、使用者識別子と指紋情報とが保存可能な指紋ＤＢと、入力された使用者識別子と採取した指紋情報とを前記指紋ＤＢと照合し、その照合結果が一致した場合、又は、前記入力された使用者識別子が前記指紋ＤＢに保存されていない場合に、前記採取した指紋情報を出力する指紋照合装置と、前記指紋照合装置から出力された指紋情報とその使用者識別子とを含む認

（ステップＳ３４）。指紋照合が一致しない場合には、もう一度指紋情報の採取を行う（ステップＳ３１）。尚、前述のステップＳ３３での指紋照合に用いるしきい値は、後述する指紋認証サーバでの指紋照合に用いるしきい値より低く設定されている。

【００３９】次に、計算機２３は、受信した指紋情報に使用者識別子等の認証に必要な情報を加えた認証情報を指紋認証サーバ２５に送信する（ステップＳ３５）。

【００４０】次に、指紋認証サーバ２５は、受信した認証情報と認証ＤＢ２４に保存されている認証情報を用いて認証を行う（ステップＳ３６）。認証成功の場合には、認証成功のレスポンスを計算機２３に送信する。認証失敗の場合には認証失敗のレスポンスを計算機２３に送信する。尚、前述のステップＳ３６の認証で行われる指紋照合に使用されるしきい値は、複数の指紋照合装置２２－１～３を一元管理するために設定されたしきい値（通常のしきい値）であり、指紋照合装置に設定されたしきい値より高く設定されたしきい値を使用する。

【００４１】次に、計算機２３は、指紋認証サーバ２５のレスポンスが認証成功の場合、アプリケーションの実行をする（ステップＳ３７）。認証失敗の場合、ユーザに通知して終了する。

【００４２】次に、計算機２３でアプリケーションが実行された場合（ステップＳ３７）、指紋照合装置２２は、指紋ＤＢ２１に該当指紋情報が保存されているかを判断する（ステップＳ３８）。保存されている場合には、終了する。保存されていない場合には、採取した指紋情報と使用者識別子を指紋ＤＢ２１に保存する（ステップＳ３９）。

【００４３】以上のように、この実施の形態のネットワーク指紋認証システムによれば、指紋照合装置での指紋照合のしきい値を、指紋認証サーバでの指紋照合のしきい値より低く設定したことにより、指紋照合認証サーバでの指紋照合で一致するはずの指紋情報が、指紋照合装置での指紋照合で失敗する可能性が低くなるので、使用者の指紋の採取の回数が少なくなり、使用者の利便性の向上が実現できる。また、既存の指紋認証サーバ側を変更する必要がなく、端末側（本実施の形態では指紋照合装置）だけの変更で適用可能である。

【００４４】実施の形態３．以上の実施の形態２では、指紋照合装置での指紋照合は一致しないが、指紋認証サーバで指紋照合させた場合に一致するような指紋を採取した場合に、指紋照合装置での照合で一致するように、指紋照合装置での照合のしきい値を低くしたものであったが、次に、指紋認証サーバでの認証が成功した最新の使用者から採取した指紋を、指紋照合装置に保存する実施の形態を示す。

【００４５】実施の形態１と同様に図１は、この発明の実施の形態３の全体的な構成を示すシステム構成図である。前述の実施の形態と同一部分の説明を省略する。この実施の形態では、指紋照合装置２２は、採取した指紋情報の指紋認証サーバ２５での指紋認証結果が認証成功である度に、当該採取した指紋情報を指紋ＤＢ２１に保存するように構成されている。

【００４６】次に、動作について図３用いて説明する。まず、指紋照合装置２２は、計算機２３の指示により使用者から指紋情報の採取を行う（ステップＳ４１）。この時に、指紋情報を採取する使用者の使用者識別子も計算機２３より受取る。そして、上記の使用者識別子を用いて指紋ＤＢ２１にアクセスして該当使用者の指紋情報が保存されているかを判断する（ステップＳ４２）。指紋情報が保存されていない場合は、計算機２３にその採取した指紋情報を送信する（ステップＳ４４）。指紋情報が保存されている場合には、その保存されている指紋情報と採取した指紋情報を照合する（ステップＳ４３）。ステップＳ４３で、指紋照合が一致した場合には、採取した指紋情報を計算機２３に送信する（ステップＳ４４）。指紋照合が一致しない場合には、もう一度指紋情報の採取を行う（ステップＳ４１）。

【００４７】次に、計算機２３は、受信した指紋情報に使用者識別子等の認証に必要な情報を加えた認証情報を指紋認証サーバ２５に送信する（ステップＳ４５）。

【００４８】次に、指紋認証サーバ２５は、受信した認証情報と認証ＤＢ２４に保存されている認証情報を用いて認証を行う（ステップＳ４６）。認証成功の場合には、認証成功のレスポンスを計算機２３に送信する。認証失敗の場合には認証失敗のレスポンスを計算機２３に送信する。

【００４９】次に、計算機２３は、指紋認証サーバ２５のレスポンスが認証成功の場合、アプリケーションの実行をする（ステップＳ４７）。認証失敗の場合、ユーザに通知して終了する。

【００５０】次に、計算機２３でアプリケーションが実行された場合（ステップＳ４７）、指紋照合装置２２は、採取した指紋情報と使用者識別子を指紋ＤＢ２１に保存する（ステップＳ４８）。

【００５１】以上のように、この実施の形態のネットワーク指紋認証システムによれば、指紋認証サーバでの指紋認証が成功した最新の指紋情報を指紋ＤＢに保存することにより、指紋照合装置での照合で失敗する可能性が低くなるので、使用者の指紋の採取の回数が少なくなり、使用者の利便性の向上が実現できる。また、既存の指紋認証サーバ側を変更する必要がなく、端末側（本実施の形態では計算機、指紋照合装置、指紋ＤＢ）だけの変更で適用可能である。

【００５２】実施の形態４．以上の実施の形態３は、指紋認証サーバでの認証が成功した最新の使用者から採取した指紋を、指紋照合装置に保存するものであったが、次に指紋認証サーバでの認証が失敗であった場合の指紋も保存し、次に指紋を採取した場合に、その失敗した指

紋と照合した結果が一致した場合には、再度指紋を採取し直す実施の形態を示す。

【００５３】実施の形態１と同様に図１は、この発明の実施の形態４の全体的な構成を示すシステム構成図である。前述の実施の形態と同一部分の説明を省略する。この実施の形態では、指紋照合装置２２は、採取した指紋情報の指紋認証サーバ２５での指紋認証結果が認証失敗であった場合に当該採取した指紋情報と入力された使用者識別子とを指紋ＤＢ２１に保存しておき、後に入力された使用者識別子が前記認証失敗となった使用者識別子である場合に前記保存した認証失敗であった指紋情報と後に採取した指紋情報とを照合し、一致する場合には当該後に採取した指紋情報を計算機２３に出力しないように構成されている。また、前記認証失敗であった指紋情報と後に採取した指紋情報とを照合する指紋照合のしきい値は、指紋認証サーバ２５で使用されるしきい値より高く設定されている。

【００５４】次に、動作について図４を用いて説明する。まず、指紋照合装置２２は、計算機２３の指示により使用者から指紋情報の採取を行う（ステップＳ５１）。この時に、指紋情報を採取する使用者の使用者識別子も計算機２３より受取る。そして、上記の使用者識別子を用いて指紋ＤＢ２１にアクセスして該当使用者の指紋情報が保存されているかを判断する（ステップＳ５２）。指紋情報が保存されていない場合は、計算機２３にその採取した指紋情報を送信する（ステップＳ５４）。指紋情報が保存されている場合には、その保存されている指紋情報と採取した指紋情報を照合する（ステップＳ５３）。ステップＳ５３で、指紋認証サーバ２５の指紋認証で認証成功となった指紋情報との指紋照合が一致した場合には、採取した指紋情報を計算機２３に送信する（ステップＳ５４）。指紋認証サーバ２５の指紋認証で認証成功となった指紋情報との指紋照合が一致しない場合、又は、指紋認証サーバ２５の指紋認証で認証失敗となった指紋情報との指紋照合が一致した場合には、もう一度指紋情報の採取を行う（ステップＳ５１）。尚、ステップＳ５３で、認証失敗の指紋情報との指紋照合に用いるしきい値は、指紋認証サーバ２５での指紋照合に用いるしきい値より高く設定されている。

【００５５】次に、計算機２３は、受信した指紋情報に使用者識別子等の認証に必要な情報を加えた認証情報を指紋認証サーバ２５に送信する（ステップＳ５５）。

【００５６】次に、指紋認証サーバ２５は、受信した認証情報と認証ＤＢ２４に保存されている認証情報を用いて認証を行う（ステップＳ５６）。認証成功の場合には、認証成功のレスポンスを計算機２３に送信する。認証失敗の場合には認証失敗のレスポンスを計算機２３に送信する。尚、前述のステップＳ５６の認証で行われる指紋照合に使用されるしきい値は、複数の指紋照合装置２２－１～３を一元管理するために設定されたしきい値（通常のしきい値）である。

【００５７】次に、計算機２３は、指紋認証サーバ２５のレスポンスが認証成功の場合、アプリケーションの実行をする（ステップＳ５７）。

【００５８】次に、指紋照合装置において計算機でアプリケーションが実行された（ステップＳ５７）場合、指紋ＤＢ２２に該当指紋情報が保存されているかを判断する（ステップＳ５８）。保存されている場合には、終了する。保存されていない場合には、採取した指紋情報と使用者識別子と認証結果を指紋ＤＢ２２に保存する（ステップ５９）。また、ステップＳ５６で認証失敗の場合には、採取した指紋情報と使用者識別子と認証結果を指紋ＤＢ２２に保存し（ステップ５９）、終了する。

【００５９】以上のように、この実施の形態のネットワーク指紋認証システムによれば、一度指紋認証サーバで認証失敗になった指紋情報と一致する指紋情報を指紋認証サーバに送らないようにすることにより、以前認証失敗となった指紋情報と同じような指紋情報は指紋認証サーバへ送信されないので、指紋認証サーバへの送信回数を軽減でき、ユーザの利便性の向上、指紋認証サーバの負荷軽減、ネットワークの通信負荷軽減を実現することができる。また、既存の指紋認証サーバ側を変更する必要がなく、端末側（本実施の形態では計算機、指紋照合装置、指紋ＤＢ）だけの変更で適用可能である。

【００６０】また、指紋認証サーバで認証失敗になった指紋情報と後に採取した指紋情報とを照合する場合に使用するしきい値を指紋認証サーバで使用するしきい値よりも高く設定したことにより、指紋認証サーバでの指紋照合で一致するはずの指紋情報を、指紋照合装置が指紋認証サーバに送らないようにする可能性を低くすることができる。すなわち、指紋認証サーバでの指紋照合で一致するはずの指紋情報を、指紋照合装置が破棄する可能性を低くすることができる。

【００６１】実施の形態５．以上のように実施の形態４は、指紋認証サーバで認証が失敗した指紋を指紋照合装置において利用して、指紋認証サーバに送信しても認証が失敗するとわかっている認証情報を送信しないものであったが、次に、指紋照合装置で照合を行った場合の照合度をユーザに提示する実施の形態を示す。

【００６２】実施の形態１と同様に図１は、この発明の実施の形態５の全体的な構成を示すシステム構成図である。前述の実施の形態と同一部分の説明を省略する。この実施の形態では、計算機２３は、採取した指紋情報と指紋ＤＢ２１に保存された指紋情報との照合度を使用者に提示可能に構成されている。

【００６３】次に動作について図２を用いて説明する。まず、指紋照合装置２２は、計算機２３の指示により使用者から指紋情報の採取を行う（ステップＳ３１）。この時に、指紋情報を採取する使用者の使用者識別子も計算機２３より受取る。そして、上記の使用者識別子を用

いて指紋ＤＢ２１にアクセスして該当使用者の指紋情報が保存されているかを判断する（ステップＳ３２）。指紋情報が保存されていない場合は、計算機２３にその採取した指紋情報を送信する（ステップＳ３４）。指紋情報が保存されている場合には、その保存されている指紋情報と採取した指紋情報を照合する（ステップＳ３３）。この時、指紋照合装置２２はその照合度を計算機２３に送信し、計算機２３はその照合度を使用者に提示する。ステップＳ３３で、指紋照合が一致した場合には、採取した指紋情報を計算機２３に送信する（ステップＳ３４）。指紋照合が一致しない場合には、もう一度指紋情報の採取を行う（ステップＳ３１）。

【００６４】次に、計算機２３は、受信した指紋情報に使用者識別子等の認証に必要な情報を加えた認証情報を指紋認証サーバ２５に送信する（ステップＳ３５）。

【００６５】次に、指紋認証サーバ２５は、受信した認証情報と認証ＤＢ２４に保存されている認証情報を用いて認証を行う（ステップＳ３６）。認証成功の場合には、認証成功のレスポンスを計算機２３に送信する。認証失敗の場合には認証失敗のレスポンスを計算機２３に送信する。

【００６６】次に、計算機２３は、指紋認証サーバ２５のレスポンスが認証成功の場合、アプリケーションの実行をする（ステップＳ３７）。認証失敗の場合、ユーザに通知して終了する。

【００６７】次に、計算機２３でアプリケーションが実行された場合（ステップＳ３７）、指紋照合装置２２は、指紋ＤＢ２１に該当指紋情報が保存されているかを判断する（ステップＳ３８）。保存されている場合には、終了する。保存されていない場合には、採取した指紋情報と使用者識別子を指紋ＤＢ２１に保存する（ステップＳ３９）。

【００６８】以上のように、この実施の形態のネットワーク指紋認証システムによれば、採取した指紋情報と指紋ＤＢに保存された指紋情報との指紋照合の照合度を使用者に提示することにより、当該使用者が指の置き方を学習するので、採取される指紋情報が安定し、サーバへの送信回数を軽減でき、ユーザの利便性の向上、指紋認証サーバの負荷軽減、ネットワークの通信負荷軽減を実現することができる。また、既存の指紋認証サーバ側を変更する必要がなく、端末側（本実施の形態では計算機、指紋照合装置）だけの変更で適用可能である。

【００６９】実施の形態６．以上のように、実施の形態５は、指紋照合装置の中で照合する場合に照合度を使用者に提示するものであったが、次に、認証ＤＢに保存されている指紋情報を変更した場合に対応できる実施の形態を示す。

【００７０】実施の形態１と同様に図１は、この発明の実施の形態２の全体的な構成を示すシステム構成図である。前述の実施の形態と同一部分の説明を省略する。この実施の形態では、指紋認証サーバ２５は、認証ＤＢ２４に保存されている指紋情報が変更された場合に、その使用者識別子と指紋削除通知とを計算機２３に送信するように構成されている。計算機２３は、指紋認証サーバ２５から指紋削除を通知された場合に指紋照合装置２２に使用者識別子と指紋削除通知を送信するように構成されている。また、指紋照合装置２２は、指紋認証サーバ２５に登録されている指紋情報が変更された場合に、指紋ＤＢ２１に保存されている指紋情報を削除するように構成されており、ここでは、計算機２３より指紋削除を通知されたされた場合に、前記使用者識別子に対応する指紋情報を指紋ＤＢ２１から削除するように構成されている。

【００７１】次に動作について図２、図５を用いて説明する。まず、指紋照合装置２２は、計算機２３の指示により使用者から指紋情報の採取を行う（ステップＳ３１）。この時に、指紋情報を採取する使用者の使用者識別子も計算機２３より受取る。そして、上記の使用者識別子を用いて指紋ＤＢ２１にアクセスして該当使用者の指紋情報が保存されているかを判断する（ステップＳ３２）。指紋情報が保存されていない場合は、計算機２３にその採取した指紋情報を送信する（ステップＳ３４）。指紋情報が保存されている場合には、その保存されている指紋情報と採取した指紋情報を照合する（ステップＳ３３）。ステップＳ３３で、指紋照合が一致した場合には、採取した指紋情報を計算機２３に送信する（ステップＳ３４）。指紋照合が一致しない場合には、もう一度指紋情報の採取を行う（ステップＳ３１）。

【００７２】次に、計算機２３は、受信した指紋情報に使用者識別子等の認証に必要な情報を加えた認証情報を指紋認証サーバ２５に送信する（ステップＳ３５）。

【００７３】次に、指紋認証サーバ２５は、受信した認証情報と認証ＤＢ２４に保存されている認証情報を用いて認証を行う（ステップＳ３６）。認証成功の場合には、認証成功のレスポンスを計算機２３に送信する。認証失敗の場合には認証失敗のレスポンスを計算機２３に送信する。

【００７４】次に、計算機２３は、指紋認証サーバ２５のレスポンスが認証成功の場合、アプリケーションの実行をする（ステップＳ３７）。認証失敗の場合、ユーザに通知して終了する。

【００７５】次に、計算機２３でアプリケーションが実行された場合（ステップＳ３７）、指紋照合装置２２は、指紋ＤＢ２１に該当指紋情報が保存されているかを判断する（ステップＳ３８）。保存されている場合には、終了する。保存されていない場合には、採取した指紋情報と使用者識別子を指紋ＤＢ２１に保存する（ステップＳ３９）。

【００７６】次に、認証ＤＢ２４の指紋情報を変更した場合の動作について図５を用いて説明する。指紋認証サ

ーバ２５は、認証ＤＢ２４に保存されている指紋情報が変更されると（ステップＳ６１）、指紋削除通知と該当使用者識別子を計算機２３に送信する（ステップＳ６２）。計算機２３は、指紋認証サーバ２５より指紋削除が通知されると指紋照合装置２２に指紋削除通知と該当使用者識別子を送信する（ステップＳ６３）。指紋照合装置２２は、計算機２３より指紋削除を通知されると、使用者識別子の指紋情報が指紋ＤＢ２１に保存されているかを検査し（ステップＳ６４）、保存されている場合には、該当情報を削除する（ステップＳ６５）。

【００７７】以上のように、この実施の形態６のネットワーク指紋認証システムによれば、認証ＤＢに保存された指紋情報が変更された場合に、指紋ＤＢの内容を削除するようにしたことにより、容易に指紋情報の整合性を保つことができる。

【００７８】実施の形態７．以上のように、実施の形態６では、認証ＤＢの指紋が変更されたときに指紋ＤＢの内容を削除するものであったが、次に指紋ＤＢの内容を一定期間で削除する実施の形態を示す。

【００７９】実施の形態１と同様に図１は、この発明の実施の形態２の全体的な構成を示すシステム構成図である。前述の実施の形態と同一部分の説明を省略する。この実施の形態では、指紋照合装置２２は、指紋ＤＢ２１に保存された指紋情報を保存してから所定時間後に削除するように構成されている。

【００８０】次に動作について図２と図６を用いて説明する。まず、指紋照合装置２２は、計算機２３の指示により使用者から指紋情報の採取を行う（ステップＳ３１）。この時に、指紋情報を採取する使用者の使用者識別子も計算機２３より受取る。そして、上記の使用者識別子を用いて指紋ＤＢ２１にアクセスして該当使用者の指紋情報が保存されているかを判断する（ステップＳ３２）。指紋情報が保存されていない場合は、計算機２３にその採取した指紋情報を送信する（ステップＳ３４）。指紋情報が保存されている場合には、その保存されている指紋情報と採取した指紋情報を照合する（ステップＳ３３）。ステップＳ３３で、指紋照合が一致した場合には、採取した指紋情報を計算機２３に送信する（ステップＳ３４）。指紋照合が一致しない場合には、もう一度指紋情報の採取を行う（ステップＳ３１）。

【００８１】次に、計算機２３は、受信した指紋情報に使用者識別子等の認証に必要な情報を加えた認証情報を指紋認証サーバ２５に送信する（ステップＳ３５）。

【００８２】次に、指紋認証サーバ２５は、受信した認証情報と認証ＤＢ２４に保存されている認証情報を用いて認証を行う（ステップＳ３６）。認証成功の場合には、認証成功のレスポンスを計算機２３に送信する。認証失敗の場合には認証失敗のレスポンスを計算機２３に送信する。

【００８３】次に、計算機２３は、指紋認証サーバ２５のレスポンスが認証成功の場合、アプリケーションの実行をする（ステップＳ３７）。認証失敗の場合、ユーザに通知して終了する。

【００８４】次に、計算機２３でアプリケーションが実行された場合（ステップＳ３７）、指紋照合装置２２は、指紋ＤＢ２１に該当指紋情報が保存されているかを判断する（ステップＳ３８）。保存されている場合には、終了する。保存されていない場合には、採取した指紋情報と使用者識別子を指紋ＤＢ２１に保存する（ステップＳ３９）。

【００８５】次に、指紋ＤＢ２１の指紋情報を変更した場合の動作について図６を用いて説明する。指紋照合装置２２は、指紋ＤＢ２１に保存されている指紋情報が、保存されてから所定時間以上経過しているかを判断する（ステップＳ７１）。所定時間以上経過していれば、指紋情報を削除する（ステップＳ７２）。この動作を所定時間間隔で実行する。

【００８６】以上のように、この実施の形態のネットワーク指紋認証システムによれば、指紋ＤＢの内容を所定時間間隔で調べて、保存してから所定時間経った古い情報を自動的に削除するようにしたことにより、認証ＤＢで指紋情報が変更された場合にも所定時間経過すれば対応できるようになる。また、指紋ＤＢに保存される情報がある程度最新の情報になることにより、指紋の情報の時間的変化に対応でき、既存の指紋認証サーバ側を変更する必要がなく、端末側（本実施の形態では計算機、指紋照合装置、指紋ＤＢ）だけの変更で適用可能である。

【００８７】実施の形態８．以上のように、実施の形態７では、指紋ＤＢの内容を所定時間後に削除するものであったが、次に、指紋認証サーバと計算機の間に、前回認証成功した送信指紋情報を使用して送られた指紋情報が正しいものであるかを検査する指紋認証キャッシュ・サーバを設置する実施の形態を示す。

【００８８】図１０はこの発明の実施の形態８の全体的な構成を示すシステム構成図である。図において、３１－１～３は、採取した指紋情報を出力する指紋照合装置である。３２－１～３は、前記指紋照合装置３１－１～３から出力された指紋情報とその使用者識別子とを含む認証情報を指紋認証キャッシュ・サーバに送信して認証依頼する計算機である。ここでは、指紋取得のための使用者への指示を行うと共に、指紋認証サーバの指紋認証結果に基づいてアプリケーションの制御を行うように構成されている。３３－１～３は、使用者識別子と指紋情報とが保存可能な指紋ＤＢである。なお、ここでは、予め使用者識別子と指紋情報とが保存されている。

【００８９】３４－１～３は、前記計算機３２－１～３から送信された認証情報に含まれた指紋情報とその使用者識別子とを前記指紋ＤＢ３３－１～３と照合し、その照合結果が一致した場合、又は、前記入力された使用者識別子が前記指紋ＤＢ３３－１～３に保存されていない

場合に、前記認証情報を出力する指紋認証キャッシュ・サーバである。また、照合結果が一致しない場合に指紋認証結果として認証失敗を前記計算機３２－１～３に送信するように構成されている。なおここでは、指紋認証サーバでの指紋認証結果が認証成功であった場合で、かつ、その使用者識別子が前記指紋ＤＢ３３－１～３に保存されていない場合に、前記使用者識別子と指紋情報とを前記指紋ＤＢ３３－１～３に保存するように構成されている。

【００９０】３５は、予め登録された使用者識別子と指紋情報とを含む認証情報が保存された認証ＤＢである。ここでは、認証の対象となる使用者の使用者識別子や指紋情報や前記アプリケーションに対するアクセス制御情報等を管理するように構成されている。３６は、前記指紋認証キャッシュ・サーバ３４－１～３から出力された認証情報と上記認証ＤＢ３６と照合し、その指紋認証結果を前記指紋認証キャッシュ・サーバ３４－１～３に送信する指紋認証サーバである。３７は、前記計算機３２－１～３と指紋認証キャッシュ・サーバ３４－１～３とを接続するネットワークである。

【００９１】次に動作について図８を用いて説明する。まず、指紋照合装置３１は、計算機３２の指示により使用者から指紋の採取を行い（ステップＳ８１）、採取した指紋情報を計算機３２に送信する（ステップＳ８２）。

【００９２】次に、計算機３２は、受信した指紋情報に使用者識別子等の認証に必要な情報を加えた認証情報を指紋認証サーバ２５に送信する（ステップＳ８３）。

【００９３】次に、指紋認証キャッシュ・サーバ３４は、受信した使用者識別子を用いて指紋ＤＢ３３にアクセスして該当使用者の指紋情報が指紋ＤＢ３３に保存されているかを判断する（ステップＳ８４）。指紋情報が保存されている場合には、その指紋情報と受信した指紋情報を照合し（ステップＳ８５）、照合が一致した場合には、指紋認証サーバ３６に認証情報を送信する（ステップＳ８６）。照合が一致しない場合には、計算機にその結果を通知して終了する。ステップＳ８４で、指紋情報が指紋ＤＢ３３に保存されていない場合には、そのまま認証情報を指紋認証サーバ３４に送信する（ステップＳ８６）。

【００９４】次に、指紋認証サーバ３４は、受信した認証情報と認証ＤＢ３５に保存されている情報を用いて認証を行う（ステップＳ８６）。認証成功の場合には、指紋認証キャッシュ・サーバ３４経由で計算機３２に認証成功のレスポンスを送信する。認証失敗の場合には認証失敗のレスポンスを指紋認証キャッシュ・サーバ３４経由で計算機３２に送信する。

【００９５】次に、計算機３２は、指紋認証サーバ３６のレスポンスに基づいて認証成功か認証失敗かを判断し（ステップＳ８７）、認証成功の場合は、アプリケーションの実行をする（ステップＳ８８）。認証失敗の場合は、ユーザに通知して終了する。

【００９６】次に、計算機でアプリケーションが実行された（ステップＳ８８）場合、すなわち、ステップＳ８６の認証が認証成功の場合に、指紋認証キャッシュ・サーバ３４は、指紋ＤＢ３３に該当指紋情報が保存されているかを判断する（ステップＳ８９）。保存されている場合には、終了する。保存されていない場合には、採取した指紋情報と使用者識別子を指紋ＤＢ３３に保存する（ステップＳ９０）。

【００９７】以上のように、この実施の形態のネットワーク指紋認証システムによれば、指紋認証キャッシュ・サーバで照合を行い、その指紋照合結果が一致した場合、又は、使用者識別子が指紋ＤＢに保存されていない場合に、指紋認証サーバで指紋認証を行うようにしたことにより、指紋認証が認証失敗になると予めわかっている場合には、指紋情報が指紋認証サーバに送信されないので、指紋認証サーバへの送信回数を軽減でき、ユーザの利便性の向上、指紋認証サーバの負荷軽減、ネットワークの通信負荷軽減を実現することができる。また、認証ＤＢで認証情報を一元管理することにより、管理コスト、認証情報の秘匿のセキュリティの向上が可能となる。また、既存のシステムは変更する必要がなく、指紋認証キャッシュ・サーバと指紋ＤＢを計算機と指紋認証サーバとの間に設置するだけで適用可能である。

【００９８】また、指紋認証サーバでの指紋認証結果が認証成功であった場合で、かつ、その使用者識別子が前記指紋ＤＢに保存されていない場合に、使用者識別子と採取された指紋情報とを前記指紋ＤＢに保存するようにしたことにより、次回以降の指紋照合において、当該使用者の指紋照合を指紋認証キャッシュ・サーバで行うことができるので、指紋認証サーバの負荷軽減を実現することができる。また、既存の指紋認証サーバ側を変更する必要がなく、端末側だけの変更で適用可能である。

【００９９】また、指紋認証キャッシュ・サーバで照合結果が一致しない場合に指紋認証結果として認証失敗を送信するように構成されたことにより、指紋照合が失敗するものは指紋認証サーバに送信されないので、指紋認証サーバの負荷軽減、ネットワークの通信負荷軽減という効果がある。

【０１００】また、計算機は、指紋認証サーバ又は指紋認証キャッシュ・サーバでの指紋認証結果に基づいてアプリケーションの制御を行うようにしたことにより、使用者に指紋認証結果に応じたアプリケーションを提供することができる。

【０１０１】

【発明の効果】以上のように、この発明のネットワーク指紋認証システムによれば、使用者識別子と指紋情報とが保存可能な指紋ＤＢと、入力された使用者識別子と採取した指紋情報とを前記指紋ＤＢと照合し、その照合結

果が一致した場合、又は、前記入力された使用者識別子が前記指紋ＤＢに保存されていない場合に、前記採取した指紋情報を出力する指紋照合装置と、前記指紋照合装置から出力された指紋情報とその使用者識別子とを含む認証情報を送信して認証依頼する計算機と、予め登録された使用者識別子と指紋情報とを含む認証情報が保存された認証ＤＢと、前記計算機から送信された認証情報と前記認証ＤＢと照合して指紋認証を行う指紋認証サーバとを備えたことにより、認証情報を一元管理できるうえ、指紋認証サーバには指紋照合が成功する可能性が高いものだけが送信されるので、認証失敗による再認証の回数を軽減でき、ユーザの利便性の向上、指紋認証サーバの負荷軽減、ネットワークの通信負荷軽減という効果がある。また、指紋認証サーバ側の変更は必要ないので、既存のネットワーク指紋認証システムへ適用する場合、端末側だけの変更で適用することができる。また、最終的には指紋認証サーバが指紋認証の判断を行うので、認証精度の整合性を保つことができる。

【０１０２】また、次の発明のネットワーク指紋認証システムによれば、前記指紋照合装置は、前記指紋認証サーバでの指紋認証結果が認証成功であった場合で、かつ、その使用者識別子が前記指紋ＤＢに保存されていない場合に、前記入力された使用者識別子と採取した指紋情報とを前記指紋ＤＢに保存するように構成されたことにより、次回以降の指紋照合において、当該使用者の指紋照合を指紋照合装置で行うことができるので、指紋認証サーバの負荷軽減を実現することができるという効果がある。

【０１０３】また、次の発明のネットワーク指紋認証システムによれば、前記指紋照合装置での指紋照合のしきい値が、指紋認証サーバでの指紋照合のしきい値より低く設定されたことにより、指紋照合認証サーバでの指紋照合で一致するはずの指紋情報が、指紋照合装置での指紋照合で失敗する可能性が低くなるので、より一層の認証失敗による再認証の回数を軽減を実現できるという効果がある。さらに、指紋認証サーバ側の変更は必要ないので、既存のネットワーク指紋認証システムへ適用する場合、端末側だけの変更で適用することができる。

【０１０４】また、次の発明のネットワーク指紋認証システムによれば、前記指紋照合装置は、前記採取した指紋情報の前記指紋認証サーバでの指紋認証結果が認証成功である度に、当該採取した指紋情報を前記指紋ＤＢに保存するように構成されたことにより、指紋ＤＢに保存された指紋情報は最新のものとなり、指紋照合装置での照合で失敗する可能性が低くなるので、使用者の指紋の採取の回数が少なくなり、使用者の利便性の向上が実現できるという効果がある。さらに、指紋認証サーバ側の変更は必要ないので、既存のネットワーク指紋認証システムへ適用する場合、端末側だけの変更で適用することができる。

【０１０５】また、次の発明のネットワーク指紋認証システムによれば、前記指紋照合装置は、前記採取した指紋情報の前記指紋認証サーバでの指紋認証結果が認証失敗であった場合に当該採取した指紋情報と入力された使用者識別子とを前記指紋ＤＢに保存し、後に入力された使用者識別子が前記認証失敗となった使用者識別子である場合に前記保存した認証失敗であった指紋情報と後に採取した指紋情報とを照合し、一致する場合には当該後に採取した指紋情報を前記計算機に出力しないように構成されたことにより、以前認証失敗となった指紋情報と同じような指紋情報は指紋認証サーバへ送信されないので、より一層の認証失敗による再認証の回数を軽減を実現できるという効果がある。さらに、指紋認証サーバ側の変更は必要ないので、既存のネットワーク指紋認証システムへ適用する場合、端末側だけの変更で適用することができる。

【０１０６】また、次の発明のネットワーク指紋認証システムによれば、前記計算機は、前記採取した指紋情報と前記指紋ＤＢに保存された指紋情報との照合度を使用者に提示可能に構成されたことにより、使用者の指置きの学習による指紋情報の安定化が期待でき、より一層の認証失敗による再認証の回数を軽減を実現できるという効果がある。また、指紋認証サーバ側の変更は必要ないので、既存のネットワーク指紋認証システムへ適用する場合、端末側だけの変更で適用することができる。

【０１０７】また、次の発明のネットワーク指紋認証システムによれば、前記指紋照合装置は、前記指紋認証サーバに登録されている指紋情報が変更された場合に、前記指紋ＤＢに保存されている指紋情報を削除するように構成されたことにより、容易に指紋情報の整合性を保つことができるので、指紋情報の変更されるネットワーク指紋認証システムにおいても、適応可能であるという効果がある。

【０１０８】また、次の発明のネットワーク指紋認証システムによれば、前記指紋照合装置は、前記指紋ＤＢに保存された指紋情報を所定時間後に削除するように構成されたことにより、認証ＤＢで指紋情報が変更された場合にも所定時間経過すれば対応できるようになるという効果がある。また、指紋認証サーバ側の変更は必要ないので、既存のネットワーク指紋認証システムへ適用する場合、端末側だけの変更で適用することができる。

【０１０９】さらにまた、次の発明のネットワーク指紋認証システムによれば、採取した指紋情報を出力する指紋照合装置と、前記指紋照合装置から出力された指紋情報とその使用者識別子とを含む認証情報を送信して認証依頼する計算機と、使用者識別子と指紋情報とが保存可能な指紋ＤＢと、前記計算機から送信された認証情報に含まれた指紋情報とその使用者識別子とを前記指紋ＤＢと照合し、その照合結果が一致した場合、又は、前記入力された使用者識別子が前記指紋ＤＢに保存されていな

い場合に、前記認証情報を出力する指紋認証キャッシュ・サーバと、予め登録された使用者識別子と指紋情報とを含む認証情報が保存された認証ＤＢと、前記指紋認証キャッシュ・サーバから出力された認証情報と上記認証ＤＢと照合して指紋認証を行う指紋認証サーバとを備えたことにより、認証情報を一元管理できるうえ、指紋認証サーバには指紋照合が成功する可能性が高いものだけが送信されるので、認証失敗による再認証の回数を軽減でき、指紋認証サーバの負荷軽減、ネットワークの通信負荷軽減という効果がある。また、既存のネットワーク指紋認証システムへ適用する場合、既存のシステムの変更は必要く、指紋認証キャッシュ・サーバと指紋ＤＢを計算機と指紋認証サーバとの間に設置するだけで適用することができる。また、最終的には指紋認証サーバが指紋認証の判断を行うので、認証精度の整合性を保つことができる。

【０１１０】また、次の発明のネットワーク指紋認証システムによれば、前記指紋認証キャッシュ・サーバは、照合結果が一致しない場合に指紋認証結果として認証失敗を送信するように構成されたことにより、指紋照合が失敗するものは指紋認証サーバに送信されないので、指紋認証サーバの負荷軽減、ネットワークの通信負荷軽減という効果がある。

【０１１１】また、次の発明のネットワーク指紋認証システムによれば、前記計算機は、前記指紋認証結果に基づいてアプリケーションの制御を行うように構成されたことにより、使用者に指紋認証結果に応じたアプリケーションを提供することができるという効果がある。

【図面の簡単な説明】

【図１】　実施の形態１～７のシステム構成を示すブロック図である。

＊【図２】　実施の形態１、２、５、６、７の動作を示すフロー図である。

【図３】　実施の形態３の動作を示すフロー図である。

【図４】　実施の形態４の動作を示すフロー図である。

【図５】　実施の形態６の動作を示すフロー図である。

【図６】　実施の形態７の動作を示すフロー図である。

【図７】　実施の形態８のシステム構成を示すブロック図である。

【図８】　実施の形態８の動作を示すフロー図である。

【図９】　従来技術のシステム構成を示すブロック図である。

【図１０】　従来技術の動作を示すフロー図である。

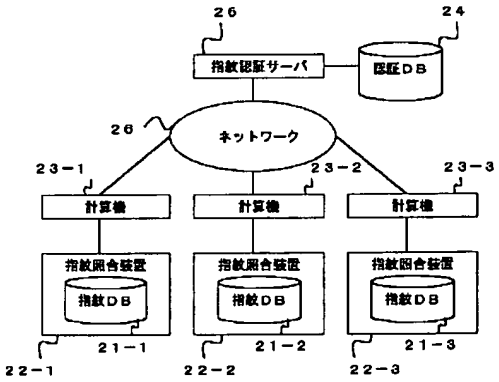
【図１１】　従来技術の動作を示すフロー図である。

【符号の説明】

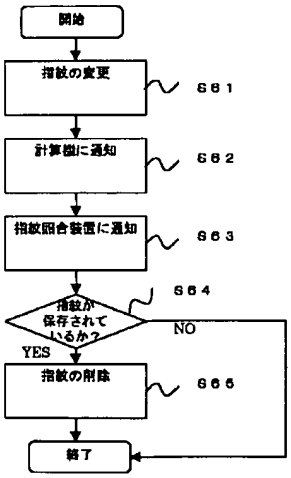
１１－１～３　コンピュータシステム　１２　通信網
１３－１～３　データ縮退ユニット　１４－１～３　特徴計測ユニット
１５－１～３　ファイルシステム　２１－１～３　指紋ＤＢ
２２－１～３　指紋照合装置　２３－１～３　計算機
２４　認証ＤＢ　２５　指紋認証サーバ
２６　ネットワーク　３１－１～３　指紋照合装置
３２－１～３　計算機　３３－１～３　指紋ＤＢ
３４－１～３　指紋認証キャッシュ・サーバ　３５　認証ＤＢ
３６　指紋認証サーバ　３７　ネットワーク

＊

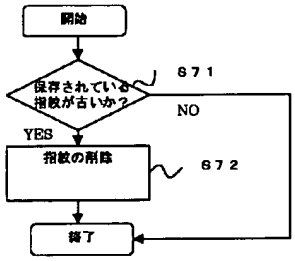
【図１】



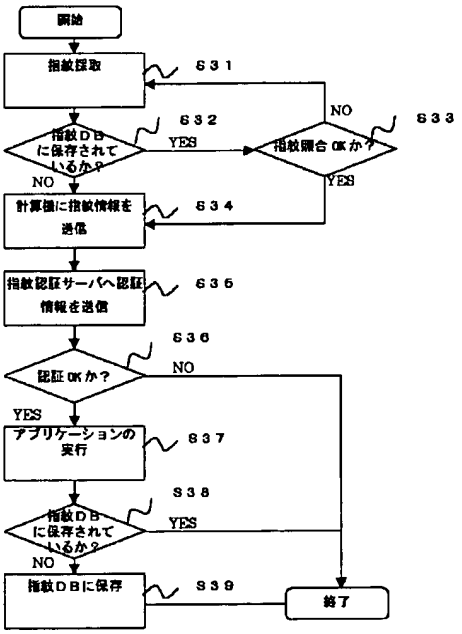
【図５】



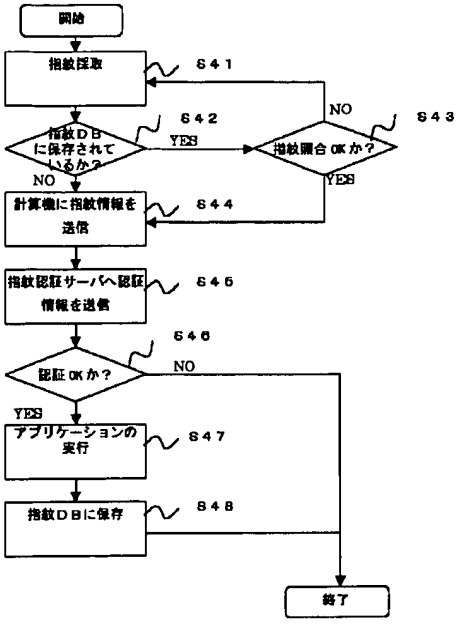
【図６】



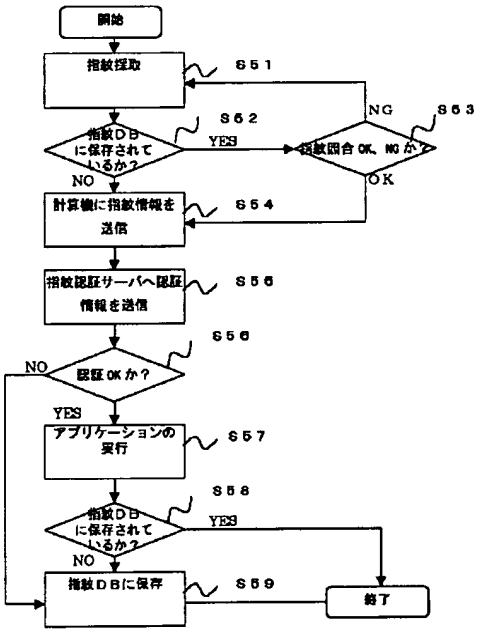
【図２】


開始
指紋採取
S31
指紋ＤＢに保存されているか？
S32
YES
NO
指紋照合 OKか？
S33
YES
NO
計算機に指紋情報を送信
S34
指紋認証サーバへ認証情報を送信
S35
認証 OKか？
S36
NO
YES
アプリケーションの実行
S37
指紋ＤＢに保存されているか？
S38
YES
NO
指紋ＤＢに保存
S39
終了

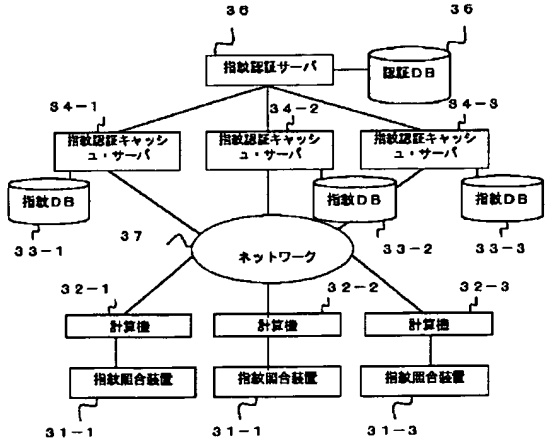
【図３】


開始
指紋採取
S41
指紋ＤＢに保存されているか？
S42
YES
NO
指紋照合 OKか？
S43
YES
NO
計算機に指紋情報を送信
S44
指紋認証サーバへ認証情報を送信
S45
認証 OKか？
S46
NO
YES
アプリケーションの実行
S47
指紋ＤＢに保存
S48
終了

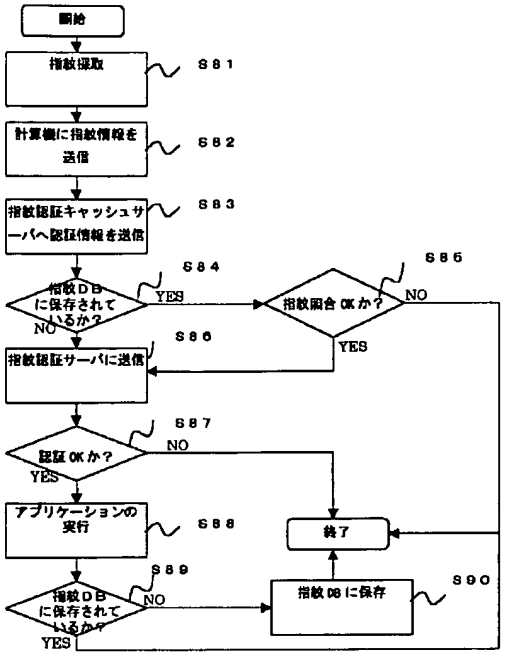
【図４】


開始
指紋採取
S51
指紋ＤＢに保存されているか？
S52
YES
NG
指紋照合 OK、NGか？
S53
OK
NO
計算機に指紋情報を送信
S54
指紋認証サーバへ認証情報を送信
S55
認証 OKか？
S56
NO
YES
アプリケーションの実行
S57
指紋ＤＢに保存されているか？
S58
YES
NO
指紋ＤＢに保存
S59
終了

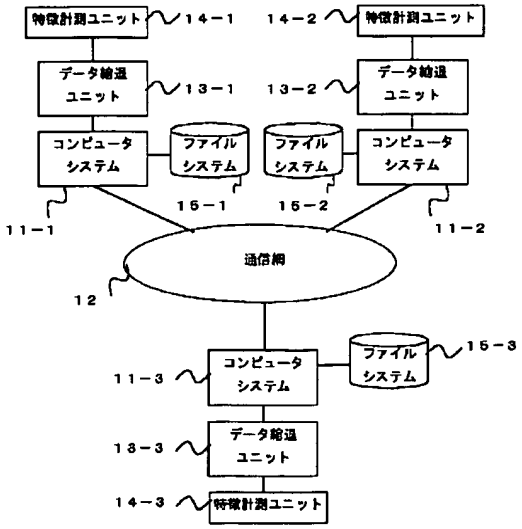
【図７】


36
36
指紋認証サーバ
認証DB
34－1
34－2
34－3
指紋認証キャッシュ・サーバ
指紋認証キャッシュ・サーバ
指紋認証キャッシュ・サーバ
指紋DB
指紋DB
指紋DB
33－1
33－2
33－3
37
ネットワーク
32－1
32－2
32－3
計算機
計算機
計算機
指紋照合装置
指紋照合装置
指紋照合装置
31－1
31－1
31－3

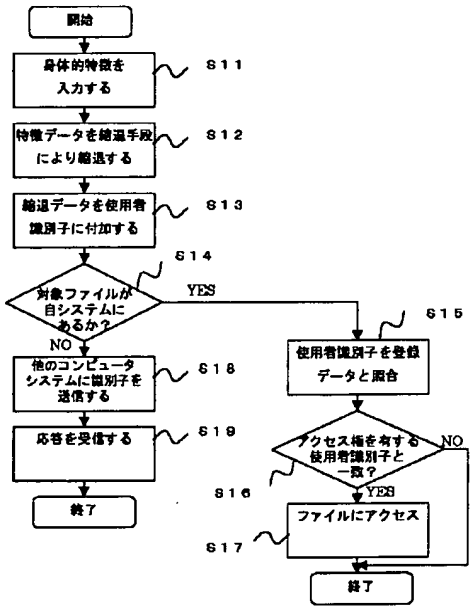
【図８】


開始
指紋採取
S81
計算機に指紋情報を送信
S82
指紋認証キャッシュサーバへ認証情報を送信
S83
S84
指紋ＤＢに保存されているか？
YES
NO
S85
指紋照合 OK か？
NO
YES
S86
指紋認証サーバに送信
S87
認証 OK か？
NO
YES
アプリケーションの実行
S88
終了
S89
指紋ＤＢに保存されているか？
NO
YES
S90
指紋 DB に保存

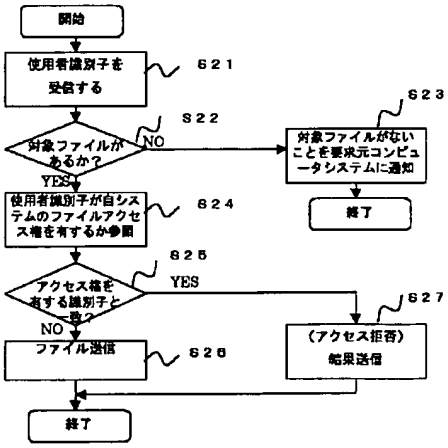
【図９】


特徴計測ユニット
14－1
14－2
特徴計測ユニット
データ縮退ユニット
13－1
13－2
データ縮退ユニット
コンピュータシステム
ファイルシステム
ファイルシステム
コンピュータシステム
15－1
15－2
11－1
11－2
通信網
12
コンピュータシステム
ファイルシステム
15－3
11－3
データ縮退ユニット
13－3
特徴計測ユニット
14－3

【図１０】


開始
身体的特徴を入力する
S11
特徴データを縮退手段により縮退する
S12
縮退データを使用者識別子に付加する
S13
S14
対象ファイルが自システムにあるか？
YES
NO
S15
使用者識別子を登録データと照合
他のコンピュータシステムに識別子を送信する
S18
応答を受信する
S19
終了
アクセス権を有する使用者識別子と一致？
NO
YES
S16
ファイルにアクセス
S17
終了

【図１１】


開始
使用者識別子を受信する
S21
S22
対象ファイルがあるか？
NO
YES
S23
対象ファイルがないことを要求元コンピュータシステムに通知
終了
使用者識別子が自システムのファイルアクセス権を有するか参照
S24
S25
アクセス権を有する識別子と一致？
YES
NO
S27
（アクセス拒否）結果送信
ファイル送信
S26
終了

フロントページの続き

(72)発明者 岡崎 直宣
東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内
(72)発明者 中村 浩
東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内
(72)発明者 藤井 照子
東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内

Ｆターム(参考) 5B043 AA09 BA02 CA05 CA09 CA10
FA02 FA03 FA07 FA08 GA01
5B085 AE02 AE26 BG07